Remarks/Arguments:

By this Amendment, Applicant has amended claims 1, 12 and 14. Applicant has also cancelled claims 17-28. Accordingly, claims 1-16 are pending.

Examiner Interview

Applicant acknowledges with appreciation the courtesies extended by Examiner Zia to the undersigned on December 21, 2004. In the course of that interview, the undersigned proposed an amendment of claim 1 to Examiner Zia which is the same amendment as included herein. Examiner Zia indicated that it was possible that this amendment would overcome the pending rejection, but that the Examiner would require a further examination. Accordingly, Applicant is filing an RCE concurrent with this Amendment.

Claim Rejections Under Section 102

Claims 1-28 stand rejected under 35 U.S.C. §102(e) as being anticipated by Chaum. By this Amendment, Applicant respectfully traverses the Section 102(e) rejection.

As noted above, claims 17-28 have been cancelled. Claims 1, 12, and 14 are independent claims. Claims 2-11 are dependent on claim 1. Claim 13 is dependent on claim 12, and claims 15-16 are dependent on claim 14.

Turning first to independent claim 1, it is directed to an equipment authentication and cryptographic communication system including user-end equipment, system-end equipment, and a key center for administering authentication of equipment in the system. The equipment authentication and cryptographic communication system includes the following features:

- the user-end equipment is provided with individual user-end equipment information issued by the key center and individual user-end equipment secret information corresponding to the individual user-end equipment's information,

and the user-end equipment transmits the individual user-end equipment information to the system-end equipment.

- the system-end equipment receives the individual user-end equipment information from the user-end equipment, **reproduces by a system conversion the individual user-end equipment secret information from the received individual user-end equipment information using an equivalent secret key cryptographic algorithm of the key center**, and authenticates the user-end equipment by confirming that the user-end equipment legitimately has the individual user-end equipment secret information by using a challenge response utilizing a common key cryptographic algorithm, and

- the user-end equipment and the system-end equipment execute a cryptographic communication with each other using the individual user-end equipment secret information.

Applicant submits that the equipment authentication and cryptographic communication system defined by claim 1 is patentably distinguished from the Chaum Patent at least based on the requirement that the system-end equipment receives the individual user-end equipment information from the user-end equipment, and reproduces by a system conversion the individual user-end equipment secret information from the received individual user-end equipment information using an equivalent secret key cryptographic algorithm of the key center (generally referred to as the "System Conversion Feature" of Applicant's claimed invention). Simply put, the Chaum Patent does not teach or suggest the System Conversion Feature defined by Applicant's claim 1, as well as the claims dependent thereon.

The System Conversion Feature is not the addition of new matter, but is based on the application as originally filed. In particular, discussions concerning the System Conversion Feature are found throughout the originally filed application, and in this regard, Applicant points, for example, to the discussion at page 23, line 2 to page 24, line 8.

In addition, the originally filed application discusses the advantages attributed to the System Conversion Feature. In this regard, Applicant points to the discussion at page 8, lines

20-24 of the originally filed application. In particular, the equipment authentication cryptographic communication system defined by claim 1 allows the system-end equipment to share the individual user-end equipment's secret information for each of the user-end equipment without storing it in a form of a data base. This enables the system-end equipment to make an authentication of legitimacy of the user-end equipment as well as cryptographic communications.

The Chaum Patent as shown in Figures 1 and 2 generally relates to outside collection stations which communicate over a short-range, high speed bi-directional microwave communication link with one or more in-vehicle units associated with vehicles on traffic lanes of a highway. At least two up-link communication sessions and at least one down-link communication session are transacted in real time during the limited duration of an outside collection station communication footprint as the vehicle travels along its lane past a highway toll plaza. In addition, a plaza computer local area network and downlink plaza controller is used to facilitate simultaneous multi-lane transactions.

The multi-lane toll plaza environment of the Chaum Patent shown in Figures 1 and 2 is discussed in detail at column 6, line 65 through to column 9, line 48. In particular, Applicant notes that the Chaum Patent at column 7, line 66 to column 8, line 4 states the following:

> The Reload Computer [40] may be installed with an interval Kryptor (a high speed RSA/DES encryption device) mounted in an ISA expansion slot. The Kryptor (a high speed RSA/DES) generates blank electronic checks and balance data tier transmission to a remote Reload Station (emphasis added).

But this recited portion of the Chaum Patent, as well as the other discussion in the Chaum Patent indicates that the Chaum system does not disclose a system reproducing individual user-end equipment secret information from received individual user-end equipment information as defined in Applicant's claim 1. Nor is there any teaching or suggestion of the system conversion of Applicant's claim 1 of reproducing the individual user-end equipment secret information from the received individual user-end equipment information using an equivalent secret key cryptographic algorithm of the key center. Thus there are very real differences between the equipment authentication cryptographic communication system defined by Applicants' claim 1 and the teaching of the Chaum Patent. Because the System Conversion Feature of Applicant's claim 1 and dependent claims 2-11 are not taught or suggested in the

Chaum Patent, Applicant requests that the 102(e) rejection directed to these claims be withdrawn.

Applicant has also amended independent claims 12 and 14 so that they too, in a similar fashion, include the System Conversion Feature of Applicant's claimed invention. Thus the remaining pending claims, 12-16 are also patentably distinguished from the Chaum Patent.

Based on the above discussion, Applicant requests that the Section 102(e) rejection directed to claims 1-16 be withdrawn.

In view of the foregoing remarks and amendments, Applicant respectfully submits that claims 1-16 are in condition for allowance. Reconsideration and allowance of all pending claims are respectfully requested.

Respectfully submitted,

Daniel N. Calder

Daniel N. Calder, Reg. No. 27,424
Attorney for Applicant

DNC/dmw/ds

Dated: January 21, 2005

P.O. Box 980
Valley Forge, PA 19482
(610) 407-0700

The Commissioner for Patents is hereby authorized to charge payment to Deposit Account No. **18-0350** of any fees associated with this communication.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, with sufficient postage, in an envelope addressed to Mail Stop BCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 21, 2005.

Daniel N. Calder

DMW_I:\MAT\V07838\AMEND02.DOC